ENGINEERING RESEARCH INSTITUTE
UNIVERSITY OF MICHIGAN
ANN ARBOR

TOPICS IN THE THEORY OF GROUP CHARACTERS

by

Walter Feit

Project 2200

DETROIT ORDNANCE DISTRICT, ORDNANCE CORPS, U.S. ARMY CONTRACT NO. DA-20-018-ORD-13281, DA Project No. 599-01-004 ORD Project NO. TB2-001-(1040), OOR Project NO. 31-124

July, 1954

PREFACE

I wish to acknowledge my indebtedness to Professor Robert M. Thrall under whom this dissertation was written. I also wish to express my thanks to Professor Richard Brauer for the interest he has shown in this work and for his many valuable suggestions.

A part of this dissertation was written under the sponsorship of the Office of Ordnance Research, U. S. Army, Contract DA-20-018-ORD 13281. Professor Robert M. Thrall was the project director.

TABLE OF CONTENTS

INTRODUCTION

Two separate problems are treated in this dissertation. The reason for including them both in one piece of work is that the methods used are very similar, in both case they lean heavily on the well known theorem of R. Brauer on the characterization of characters (see [4] or [9]).

The first problem is a question in the theory of modular characters. If B is a p-block of defect d, then it has been conjectured that the number of characters in B is at most p^d. R. Brauer has proved this result for $d = 0, 1,$ or 2. He has furthermore shown that the number of characters in B is always bounded by

$$p^{\frac{d(d+1)}{2}}$$

(see [3]). This bound is improved in this dissertation; it is here shown that the number of characters in B cannot exceed

$$\left[\frac{p^{2d}}{4}\right] + 1,$$

where $[a]$ denotes the greatest integer less than or equal to a.

The second problem treated here is a question on the structure theory of groups. Suppose that $\mathfrak{G}$ is a group of order $g = mq$, with $(m,q) = 1$. Let $\mathfrak{M}$ denote the set of all elements in $\mathfrak{G}$ whose order divides m. In 1907 G. Frobenius proved that the number of elements in $\mathfrak{M}$ is divisible by m; he furthermore conjectured that if $\mathfrak{M}$ contains exactly m elements, then $\mathfrak{M}$ is a normal subgroup of $\mathfrak{G}$, (see [7]). Frobenius was unable to prove his conjecture, but he proved that $\mathfrak{M}$ is a normal subgroup under the additional hypotheses that $\mathfrak{G}$ contains a subgroup $\mathfrak{Q}$ of order q which is its own normalizer, and which is disjoint from all its conjugates. In this dissertation the theorem is proved without the hypothesis that $\mathfrak{Q}$ is its own normalizer.

The important thing is not so much that a more general theorem is proved, but the fact that a very different method of proof is used. Frobenius' original proof was very ingenious, and consequently almost impossible to generalize. The methods used here might lead to a better understanding of the theorem, and possibly might be extendable to a proof of the full conjecture.

CHAPTER I

1. Representations and Characters.[1]

A representation Z of a finite group $\mathcal{G}$ of order g is a homomorphism of $\mathcal{G}$ into a set of non-singular z by z matrices with complex coefficients,

$$G \longrightarrow Z(G);$$

z is called the degree of Z. Such a representation Z is said to be irreducible if no proper subspace of the underlying vector space is left invariant by all the matrices Z(G), as G ranges over the group $\mathcal{G}$. Two representations Z and Z' are considered equivalent, if there exists a non-singular matrix P with the property that

$$P\,Z(G)P^{-1} = Z'(G)$$

for all G in $\mathcal{G}$.

For a given (irreducible) representation Z, let the function χ be defined on $\mathcal{G}$ by the following,

$$\chi(G) = \text{the trace of } Z(G), \text{ for each } G \text{ in } \mathcal{G}.$$

χ is called an (irreducible) character of the group $\mathcal{G}$. Sometimes, when convenient, we will also call χ the character of the representation Z. As each characteristic root of Z(G) is a g^{th} root of unity, $\chi(G)$ is a sum of z roots

[1] For the material in this section see for instance [6].

of unity. In particular $\chi(G)$ is always an algebraic integer. $\chi(1) = z =$ degree of Z, z is also called the degree of χ.

An immediate consequence of the definition is that the characters χ_1 and χ_2 of two equivalent representations Z_1 and Z_2 are identical. Similarly it may be shown that χ must be a class function from $\mathcal{G}$ into the complex numbers, in other words

$$\chi(G) = \chi(HGH^{-1})$$

for all G,H in $\mathcal{G}$.

If k is the class number of the group $\mathcal{G}$, then it can be shown that the number of inequivalent irreducible representations of $\mathcal{G}$ is exactly k. We will denote these by $Z_1, \ldots Z_k$ and the corresponding characters by $\chi_1, \ldots \chi_k$. We will use the convention that $\chi_1(G) = 1$ for all G in $\mathcal{G}$, this being the character of the representation Z_1 of degree 1 defined by

$$Z_1(G) = (1)$$

for all G in $\mathcal{G}$.

The following properties of representations and characters will be used later on.[2]

Theorem 1.1: *If Z is any representation of $\mathcal{G}$, then there exists a representation Z' which is similar to Z and which has the property that each matrix $Z'(G)$ is unitary. Furthermore there exists a non-singular matrix P with the property that*

[2]Most of these theorems may be found in [11], Chapter 17, as well as in [6].

$$Z(G) = P \begin{pmatrix} Z_{i_1}(G) & & & 0 \\ & \cdot & & \\ & & \cdot & \\ 0 & & & Z_{i_r}(G) \end{pmatrix} P^{-1}$$

for all G in $\mathfrak{g}$, where $Z_{i_1}, \ldots Z_{i_r}$ are irreducible representations of $\mathfrak{g}$.

Theorem 1.2: It is possible to find k inequivalent irreducible representations $Z_1, \ldots Z_k$ of $\mathfrak{g}$, such that all the coefficients of every $Z_\mu(G)$ lie in an algebraic number field K. K may be so chosen that K contains all the g^{th} roots of unity.[3]

From here on, the term representation will always mean a representation Z such that all the coefficients of each $Z(G)$ lie in the field K of Theorem 1.2.

The equations in the next two theorems are sometimes called the orthogonality relations for characters.

Theorem 1.3:

$$(1) \qquad \sum_{\mathfrak{g}} \chi_\mu(G)\,\overline{\chi_\nu(G)} = g\,\delta_{\mu\nu},$$

where $\delta_{\mu\nu}$ equals 1 or 0 accordingly as $\mu = \nu$ or not, and the bar denotes complex conjugate. The symbol $\sum_{\mathfrak{g}}$ means summation over all G in $\mathfrak{g}$.

Corollary 1.4: Any two representations which have the same character are equivalent.

---

[3]It has been proved by R. Brauer that it is possible to pick K to be the field generated by the g^{th} roots of unity. For a comparatively simple proof of this, see [9].

Theorem 1.5:

$$(2) \quad \sum_{\mu=1}^{k} \chi_\mu(G)\, \overline{\chi_\mu(H)} = \frac{g}{h(G)} \quad \text{if } G \text{ is conjugate to } H$$

$$= 0 \quad \text{if } G \text{ is not conjugate to } H,$$

where $h(G)$ denotes the number of elements of $\mathcal{G}$ which are conjugate to G.

Corollary 1.6:

$$(3) \quad \sum_{\mu=1}^{k} z_\mu \chi_\mu(G) = g \quad \text{if } G = 1$$

$$= 0 \quad \text{if } G \neq 1.$$

We conclude this section by proving the following theorem of Frobenius.

Theorem 1.7: If the function χ is the sum of irreducible characters, then there is a representation Z with χ as its character. The kernel of the representation Z is the set of all G in $\mathcal{G}$ such that $\chi(G) = \chi(1) = z$. In particular this set is a normal subgroup of $\mathcal{G}$.

Proof: $\chi = \sum_{\mu=1}^{k} a_\mu \chi_\mu$, where each a_μ is a non-negative (rational) integer. Hence χ is the character of the representation Z defined by

$$Z(G) = \begin{pmatrix} Z_1(G) & & 0 \\ & \ddots & \\ 0 & & Z_k(G) \end{pmatrix}$$

for all G in $\mathcal{G}$, where Z_μ occurs with multiplicity a_μ.

As was remarked earlier, $\chi(G)$ is a sum of z roots of unity, therefore

$$|\chi(G)| \leq z,$$

and the equality can only hold if $\chi(G)$ is z times the same root of unity ε, $\chi(G) = z\varepsilon$. Now if $\chi(G) = z$, then certainly $|\chi(G)| = z$, hence $z = \chi(G) = z\varepsilon$. Therefore $\varepsilon = 1$. This states that all the characteristic roots of $Z(G)$ are equal to 1. By Theorem 1.1, $Z(G)$ is similar to a unitary matrix and is thus diagonalizable, therefore $Z(G) = I_z$, where I_z denotes the z by z identity matrix.

Conversely if $Z(G) = I_z$, then $\chi(G) = z$. Hence G is in the kernel of Z if and only if $\chi(G) = z$, as was to be proved.

2. The Regular Representation.

Consider the permutation $\pi(H)$ acting on $\mathcal{G}$ defined by

$$\pi(H) = \begin{pmatrix} G \\ HG \end{pmatrix}$$

for all G in $\mathcal{G}$. Writing $\pi(H)$ as a g by g dimensional permutation matrix $L(H)$, we see immediately that

$$H \longrightarrow L(H)$$

is a homomorphism of $\mathcal{G}$ into a set of matrices with rational integral coefficients. In other words L is a representation of $\mathcal{G}$. The character χ of L is easily computed to have the values

$$\chi(1) = g$$
$$\chi(G) = 0 \text{ if } G \neq 1.$$

Hence by corollaries 1.4 and 1.6 we have that there exists a non-singular matrix P with the property that

$$(4) \qquad L(G) = P \begin{pmatrix} Z_1(G) & & 0 \\ & \ddots & \\ 0 & & Z_k(G) \end{pmatrix} P^{-1}$$

for all G in $\mathcal{G}$, where Z_μ occurs with multiplicity z_μ.

The representation L is called the <u>left regular representation</u>. In the same way it is possible to define the <u>right regular representation</u> R. It is clear that R and L have the same character and hence by corollary 1.4 are equivalent. We will from here on only consider L and call it <u>the regular representation of</u> $\mathcal{G}$.

3. Generalized Characters.

As there are k classes in $\mathcal{G}$ and as there are exactly k irreducible characters which are linearly independent by Theorem 1.3, it follows that every class function θ on $\mathcal{G}$ is a linear combination of the irreducible characters. In Chapters II and III below we will be interested in investigating certain arithmetical properties of class functions. For this purpose it is necessary to have a more refined concept than "linear combination".

We will define a function θ on the group $\mathcal{G}$ to be a <u>generalized character</u>, if θ is a linear combination of irreducible characters with rational integral coefficients. It is clear from this definition that θ is a class function. It is also easy to prove,

<u>Lemma 3.1</u>: <u>The set of generalized characters forms a ring</u>.

Proof: It is quite clear that the set is an additive abelian group. The only thing that needs to be proved is that the product of two generalized characters is a generalized character. By the definition it suffices to show that the product of two irreducible characters is a generalized character. This however is a trivial consequence of the fact that the product of two irreducible characters is the character of the Kronecker product of the representations associated with the given characters.

Before stating the next theorem we need to make the following definition. A subgroup $\mathfrak{E}$ of $\mathfrak{G}$ is called an *elementary group* if it is the direct product $\mathfrak{A} \times \mathfrak{P}$ of a cyclic group $\mathfrak{A}$ and a p-group $\mathfrak{P}$ such that the prime p does not divide the order of $\mathfrak{A}$. It is important to note that the definition of $\mathfrak{E}$ implies that $\mathfrak{P}$ is in the centralizer of $\mathfrak{A}$.

We are now in a position to state the fundamental theorem on generalized characters due to R. Brauer.[4]

Theorem 3.2. *A complex valued function* θ *defined on* $\mathfrak{G}$ *is a generalized character of* $\mathfrak{G}$ *if and only if the following two conditions are satisfied.*

(I) θ *is a class function.*

(II) *For every elementary subgroup* $\mathfrak{E}$ *of* $\mathfrak{G}$, *the restriction of* θ *to* $\mathfrak{E}$ *is a generalized character of* $\mathfrak{E}$.

Combining Theorem 3.2 with the orthogonality relations, we get as an immediate consequence,

Theorem 3.3: *A complex valued function* θ *defined on* $\mathfrak{G}$

---

[4]See [4], p. 357. An alternative proof may be found in [9].

is an irreducible character of $\mathfrak{G}$ if and only if, besides conditions (I) and (II) of Theorem 2.2, the following further conditions are satisfied.

(III) $\theta(1)$ is positive.

(IV) $\sum_{\mathfrak{G}} \theta(G)\overline{\theta(G)} = g.$

4. Modular Representations.

In recent years the theory of modular characters has been thoroughly developed. However we will only be interested here in the basic definitions and results.[5]

A modular representation is defined in essentially the same manner as an ordinary representation, namely a homomorphism of the group $\mathfrak{G}$ into a set of matrices with coefficients in a suitable modular field. Equivalence of two such representations is defined as for ordinary representations, except that the transforming matrix P must have its coefficients in the modular field under consideration. The term representation will always mean a representation with coefficients in the field K. Whenever we wish to talk about modular representation we will write the word modular. Modular characters are not defined in quite the same way as ordinary characters, and we postpone their definition until the next section.

A modular representation Z is said to be indecomposable if it is impossible to write the underlying vector space as a direct sum of two vector spaces, each of which is left invariant by all the matrices $Z(G)$. The modular

[5]This section and the two succeeding sections follow the treatment in [5] very closely.

representation Z is said to be irreducible if (as in the case of ordinary representations) the underlying vector space contains no invariant subspace. Clearly an irreducible representation is indecomposable. Theorem 1.1 states that in the case of ordinary representations the converse is also true. This is no longer true for modular representations and the two concepts no longer coincide in this case.

Let p be a fixed rational prime number, and let $\mathfrak{p}$ be a prime ideal in the ring of integers $\mathfrak{o}$ lying in K,[6] such that $\mathfrak{p}$ divides p. Let $\mathfrak{o}_{\mathfrak{p}}$ be the ring of all local integers with respect to $\mathfrak{p}$ lying in K, i.e. the ring of numbers $\frac{\sigma}{\tau}$, where σ is an integer in K and τ is an integer in K not divisible by $\mathfrak{p}$. The quotient field $\frac{\mathfrak{o}_{\mathfrak{p}}}{\mathfrak{p}}$ will be denoted by $\overline{K}$, this is of course identical with the field $\frac{\mathfrak{o}}{\mathfrak{p}}$. In general we will denote the residue class of an element σ in $\mathfrak{o}_{\mathfrak{p}}$ by $\overline{\sigma}$. It is possible to write the irreducible representations $Z_1, \ldots Z_k$ in such a way, that all the coefficients of each $Z_\mu(G)$ are local integers. Replacing each coefficient in $Z_\mu(G)$ by its residue class yields a matrix $\overline{Z_\mu(G)}$. It is then possible to write

$$\overline{Z_\mu(G)} = P \begin{pmatrix} F_{i_1}(G) & & 0 \\ & \ddots & \\ * & & F_{i_r}(G) \end{pmatrix} P^{-1}$$

for each G in $\mathfrak{G}$, where P is some non-singular matrix, and where $F_{i_1}, \ldots F_{i_r}$ are modular irreducible representations of $\mathfrak{G}$. The symbol $*$ under the diagonal denotes

[6] For the definition of K see Theorem 1.2.

elements about which we know nothing. If F_i occurs above with multiplicity $d_{\mu i}$, then from now on we will write

$$(5) \qquad Z_\mu \longleftrightarrow \sum_i d_{\mu i} F_i .$$

The rational integers $d_{\mu i}$ are called the <u>decomposition numbers</u> of $\mathcal{G}$.

If $\bar{L}$ denotes the left regular representation as defined in Section 2, only now considered with coefficients in $\bar{K}$, then it is still possible to show that $\bar{L}$ is equivalent to the modular right regular representation $\bar{R}$. Once again we will only consider the modular left regular representation $\bar{L}$.

Let $U_1, \ldots U_{k'}$ be the distinct indecomposable constituents of $\bar{L}$. Each U_i may be written in the form

$$U_i = \begin{pmatrix} F_i & & & & & 0 \\ & \cdot & & & & \\ & & \cdot & & & \\ & & & F^* & & \\ & * & & & \cdot & \\ & & & & \cdot & \\ & & & & & F_i \end{pmatrix}$$

if the notation is suitably chosen. Furthermore, no two of the modular irreducible representations F_i picked out in this way are equivalent, and every modular irreducible representation of $\mathcal{G}$ is equivalent to one of the F_i.

We will denote the degree of U_i by u_i, and that of F_i by f_i. Then U_i occurs in $\bar{L}$ with multiplicity f_i and F_i occurs with multiplicity u_i.

An important concept in the theory of modular representations is that of <u>Cartan invariants</u> c_{ij}. These numbers are defined as follows, c_{ij} is the multiplicity with which

F_j occurs in U_i, in other words

$$(6) \qquad U_i \longleftrightarrow \sum_j c_{ij} F_j.$$

The c_{ij} are rational non-negative integers. They are related to the decomposition numbers $d_{\mu i}$ by the equation[7]

$$(7) \qquad c_{ij} = \sum_{\mu=1}^{k} d_{\mu i}\, d_{\mu j},$$

in particular $c_{ij} = c_{ji}$. This may be written in matrix form as

$$(8) \qquad C = D'D$$

where $D = (d_{\mu i})$, D' is the transpose of D, and $C = (c_{ij})$.

There exists a representation (U_i) of $\mathfrak{g}$ in K, which if taken (mod $\mathfrak{p}$) is similar to $U_i, \overline{(U_i)} = U_i$. This with the above relations then implies that

$$(9) \qquad (U_i) \longleftrightarrow \sum_{\mu=1}^{k} d_{\mu i}\, Z_\mu .$$

5. Modular Characters.

Before proceeding to a discussion of modular characters it is necessary to make the following definitions.[8]

An element G of $\mathfrak{g}$ is called p-regular if the order of G is prime to p; an element G of $\mathfrak{g}$ which is not p-regular is said to be p-singular. It is possible to write every element G in $\mathfrak{g}$ as the product of two commuting elements AB such that A is p-regular and the order of B is a power of p. If F is a modular representation of $\mathfrak{g}$, then

[7] See [1] p. 117.

[8] See [5] pp. 561-563 for the material in this section.

the characteristic roots of $F(B)$ are all 1, as they are p^{α}th roots of unity in a field of characteristic p. Hence $F(AB)$ and $F(A)$ have the same characteristic roots and these are all g'th roots of unity, where

(10) $$g = p^{\alpha} g', \quad \text{with} \quad (p, g') = 1.$$

If A is a p-regular element of $\mathfrak{G}$, then the characteristic roots of $F(A)$ are g'th roots of unity in $\overline{K}$ (the g'th roots of unity lie in $\overline{K}$ by the choice of K). There is a unique g'th root of unity in K whose residue class coincides with any given g'th root of unity in $\overline{K}$. We will now define the <u>modular character</u> φ of F as a function on the p-regular elements G of $\mathfrak{G}$, by letting $\varphi(G)$ be the sum of the roots of unity in K corresponding to the characteristic roots of $F(G)$, $\varphi(G)$ is not defined if G is p-singular. It is important to note that $\varphi(G)$ is a number in K, not in $\overline{K}$. Actually $\varphi(G)$ is an algebraic integer for every p-regular element G in .

Let φ_i denote the modular character of the modular representation F_i, and Φ_i the character of the modular representation U_i. The modular character Φ_i is also the character of the ordinary representation (U_i) defined in equation (9) as long as the values are restricted to p-regular elements of $\mathfrak{G}$. It can be shown that the character of (U_i) vanishes for all p-singular elements of $\mathfrak{G}$, hence we can extend the definition of Φ_i by

(11) $$\Phi_i(G) = 0 \text{ if } G \text{ is p-singular.}$$

Now Φ_i may be considered as an ordinary character.

If Φ_i is restricted to a p-Sylow group $\mathfrak{P}$ of $\mathfrak{G}$, equation (11) states that $\Phi_i(G) = 0$ for all elements G of $\mathfrak{P}$ except for $G = 1$. Hence

$$(12) \qquad \sum_{\mathfrak{P}} \Phi_i(G) = \Phi_i(1) = u_i .$$

By Theorem 1.3, the order p^{α} of the group $\mathfrak{P}$ must divide the sum on the left of (12), hence p^{α} divides u_i = degree of U_i.

From the relations (6), (7) and (9) it is now possible to derive

$$(13) \qquad \Phi_i(G) = \sum_{\mu=1}^{k} d_{\mu i} \chi_{\mu}(G)$$

for all G in $\mathfrak{G}$, and

$$(14) \qquad \chi_{\mu}(G) = \sum_{i=1}^{k'} d_{\mu i} \varphi_i(G)$$

$$(15) \qquad \Phi_j(G) = \sum_{i=1}^{k'} c_{ij} \varphi_i(G)$$

where these last two relations hold for all p-regular elements G of $\mathfrak{G}$.

In analogy to Theorem 1.3, the following can be proved.

$$(16) \qquad \sum_{\mathfrak{G}} \Phi_i(G) \overline{\Phi_j(G)} = g c_{ij} .$$

$$(17) \qquad \sum_{\mathfrak{G}}' \varphi_i(G) \overline{\Phi_j(G)} = g \;{}_{ij} .$$

where $\sum_{\mathfrak{G}}'$ denotes that the sum ranges over all p-regular elements G in $\mathfrak{G}$.

We will in general now use the convention that $\sum_{\mathfrak{A}}'$ denotes summation over all p-regular elements in the set $\mathfrak{A}$.

It can be shown that the matrix $C = (c_{ij})$ is non-singular. Let $(\gamma_{ij}) = C^{-1}$, then it can easily be proved that

$$(18) \qquad \Sigma'_{\mathcal{G}}\ \varphi_i(G)\,\overline{\varphi_j(G)} = g\gamma_{ij}.$$

An immediate consequence of equation (18) is the fact that,

<u>Theorem 5.1:</u> <u>The number of p-regular elements in</u> $\mathcal{G}$ <u>is</u> $g\gamma_{11}$.

One further result that will be of some use is the fact that the number k' of inequivalent modular characters is equal to the number of classes of p-regular elements in $\mathcal{G}$. As in the case of ordinary characters we will let φ_1 denote the character of the representation F_1, where F_1 is defined by $F_1(G) = 1$ for all G in $\mathcal{G}$. Hence $\varphi_1(G)=1$ for all p-regular elements of $\mathcal{G}$.

6. <u>Blocks of Characters</u>.

Define the elements

$$(19) \qquad \Omega = \Sigma\, G$$

where the sum ranges over all G in some fixed class of $\mathcal{G}$. It is easy to show that the elements of this type form a basis for the center of the group algebra of $\mathcal{G}$. By Schur's Lemma, one immediately has that

$$(20) \quad Z_\mu(\Omega) = \omega_\mu(G)I, \qquad F_i(\Omega) = \psi_i(G)I,$$

where $\omega_\mu(G)$ is in K and $\psi_i(G)$ is an element of $\overline{K}$. It is easy to show that

$$(21) \qquad \omega_\mu(G) = \frac{h(G)\,\chi_\mu(G)}{z_\mu} \quad \text{and}$$

$$\psi_i(G) \equiv \frac{h(G)\varphi_i(G)}{f_i} \pmod{\mathfrak{p}},$$

the second equation is defined only for p-regular elements of $\mathfrak{G}$.

It can further be proved that $\omega_\mu(G)$ is always an algebraic integer.

Two modular irreducible representations F_i and F_j are said to belong to the same block B if $\psi_i(G) = \psi_j(G)$ for all G in $\mathfrak{G}$, in other words if the two representations coincide on the center of the group algebra. We will say that one of the modular indecomposable representations U_i belongs to a block B if the corresponding F_i does. Finally, an ordinary irreducible representation Z_μ is said to belong to the block B if some F_i occurring in (5) as a constituent of Z_μ belongs to B, in other words if $d_{\mu i} \neq 0$ for some F_i in B. A (modular) character χ_μ, φ_i or Φ_i is said to belong to a block B precisely when the corresponding (modular) representation Z_μ, F_i or U_i is in B.

It can be shown that if any modular indecomposable representation U_i belongs to B, then so does every constituent Z_μ of (U_i). If Z_μ belongs to B, then so does every modular irreducible constituent F_i of $\overline{Z_\mu}$. These remarks may be formulated in a slightly different manner as follows.

Theorem 6.1: If $d_{\mu i} \neq 0$, then χ_μ, φ_i and Φ_i all belong to the same block. If $c_{ij} \neq 0$ or if $\gamma_{ij} \neq 0$, then φ_i and φ_j and hence Φ_i and Φ_j belong to the same block.

As a further consequence of the above remarks it is possible to prove the following

Theorem 6.2: *Two irreducible characters* χ_μ *and* χ_ν *belong to the same block* B *if and only if*

$$(22) \qquad \omega_\mu(G) \equiv \omega_\nu(G) \pmod{\mathfrak{p}}$$

for every element G *in* $\mathfrak{g}$. *A modular irreducible character* φ_i *belongs to the same block as* χ_μ *if and only if*

$$(23) \qquad \omega_\mu(G) \equiv \psi_i(G) \equiv \frac{h(G)\varphi_i(G)}{f_i} \pmod{\mathfrak{p}}$$

for all p-regular elements G *of* $\mathfrak{g}$.

We will denote the block B containing χ_1, and hence φ_1, by B_1.

An important concept associated with the block is the idea of a defect. Suppose that $p^{\alpha - d}$ is the highest power of p which divides the degree of every character χ_μ in the block B, then d is said to be the *defect of the block* B. It can be shown that $p^{\alpha - d}$ is also the highest power of p dividing the degree of every modular irreducible character φ_i in B.

The defect d of a block B is always a non-negative integer, as the degree z_μ of every irreducible character divides g. The defect of the block B_1 is α .

CHAPTER II

7. Statement of the Problem.

In most of this chapter we will confine ourselves to the study of characters in a fixed block B of defect d. Let x denote the number of irreducible characters in B. Brauer and Nesbitt have shown[9] that

$$(24) \qquad y \leq x$$

and the equality sign holds only when $d = 0$. In this case

$$x = y = 1.$$

The main question treated in this chapter is that of finding an upper bound for the number of irreducible characters x in the block B. It has been conjectured[10] that

$$x \leq p^d.$$

Brauer has proved this conjecture for $d = 0$, 1, or 2. He has also shown[10] that in general

$$x \leq p^{\frac{d(d+1)}{2}}.$$

Our object here is to improve this bound. In Section 9 we prove the following.[11]

---

[9]See [5] p. 572.

[10]See [3] p. 218.

[11]This result is due to Professor Brauer, my original result was Theorem 9.2 (I).

Theorem 7.1: The number of irreducible characters x in a block B of defect d satisfies the inequality

$$x \leq \left[\frac{p^{2d}}{4}\right] + 1 \tag{25}$$

where $[a]$ denotes the greatest integer less than or equal to a.

In the process of proving this theorem we are able to characterize those characters lying in the block B. Also we get other bounds for x involving the numbers γ_{ii}.

In Section 10 we use the same methods necessary to prove Theorem 7.1 in proving a theorem on the decomposition of the product of two characters.

8. A Characterization of Characters in a Block.

Consider the class functions $\theta_i, i=1, \ldots k'$ defined by

$$\begin{aligned} \theta_i(G) &= p^{\alpha}\varphi_i(G) && \text{if } G \text{ is p-regular} \\ &= 0 && \text{if } G \text{ is p-singular} \end{aligned} \tag{26}$$

It can be shown,[12] using Theorem 3.2, that θ_i is a generalized character. One can now write

$$\theta_i(G) = \sum_{\mu=1}^{k} a_{\mu i}\chi_\mu(G) \tag{27}$$

for all G in $\mathfrak{G}$, where $a_{\mu i}$ is a rational integer for $\mu = 1, \ldots k$, $i = 1, \ldots k'$. Using the orthogonality relations for characters, it can easily be shown that

$$a_{\mu i} = \frac{1}{g}\sum_{\mathfrak{G}} \overline{\theta_i(G)}\,\chi_\mu(G). \tag{28}$$

From the definition (27) of θ_i, it follows that

---

[12]See [4] p. 374.

$$(29) \qquad a_{\mu i} = \frac{p^{\alpha}}{g} \sum\nolimits'_{\mathcal{G}} \overline{\varphi_i(G)}\, \chi_\mu(G)$$

$$= \frac{1}{g'} \sum\nolimits'_{\mathcal{G}} \overline{\varphi_i(G)}\, \chi_\mu(G).$$

This may be rewritten as

$$(30) \qquad \frac{g' a_{\mu i}}{z_\mu} = \sum\nolimits'_{\mathcal{G}} \overline{\varphi_i(G)} \; \frac{h(G)\chi_\mu(G)}{z_\mu}$$

$$= \sum\nolimits'_{\mathcal{G}} \overline{\varphi_i(G)}\, \omega_\mu(G),$$

where now the summation ranges over the p-regular classes of $\mathcal{G}$, not the p-regular elements. Equation (30) shows that $\frac{g' a_{\mu j}}{z_\mu}$ is a rational integer, as each term on the right is an algebraic integer, and the number is obviously rational.

In the same way, one shows that

$$(31) \qquad \frac{g\,\gamma_{ij}}{f_j} = \sum\nolimits'_{\mathcal{G}} \overline{\varphi_i(G)} \; \frac{h(G)\,\varphi_j(G)}{f_j}$$

is a rational integer. (The summation in (31) again extends over the p-regular classes in $\mathcal{G}$.)

We prove the following

Theorem 8.1: *The rational numbers* $\frac{a_{\mu i}}{z_\mu}$ *and* $p^{\alpha}\frac{\gamma_{ij}}{f_j}$ *are both local integers with respect to* p. *If* χ_μ, φ_i *and* φ_j *are in the same block* B, *then*

$$(32) \qquad \frac{a_{\mu i}}{z_\mu} \equiv \frac{p^{\alpha}\gamma_{ij}}{f_j} \pmod{p}.$$

If φ_i *is in* B *such that* $p^{\alpha-d+1}$ *does not divide* f_j, *then*

$$(33) \qquad \frac{a_{\mu i}}{z_\mu} \not\equiv 0 \pmod{p}$$

for all χ_μ *in* B. *In particular* $a_{\mu i} \neq 0$ *if and only if* χ_μ *is in* B.

Proof: As $\frac{g'a_{\mu i}}{z_\mu}$ and $\frac{g\gamma_{ij}}{f_i}$ are rational integers, division by g' yields that $\frac{a_{\mu i}}{z_\mu}$ and $p^\alpha\frac{\gamma_{ij}}{f_j}$ are local integers. If χ_μ and φ_j are in the same block, then it follows from (23) that

$$(34) \qquad \frac{g\gamma_{ij}}{f_j} \equiv \sum\nolimits_{\mathfrak{g}}' \overline{\varphi_i(G)}\ \frac{h^*(G)\ \varphi_j(G)}{f_j}$$

$$\equiv \sum\nolimits_{\mathfrak{g}}' \varphi_i(G)\,\omega_\mu(G)$$

$$\equiv \frac{g'a_{\mu i}}{z_\mu} \pmod{\mathfrak{p}}.$$

As both extreme expressions in (34) are rational, division by g' gives the required result (32).

To prove the relation (33) it is sufficient by (32) to show that if $p^{\alpha-d+1}$ does not divide f_i, then

$$(35) \qquad \frac{p^\alpha\gamma_{ij}}{f_j} \not\equiv 0 \pmod{p}.$$

Suppose on the contrary, that (35) is false. Then (32) implies that $\frac{a_{\mu i}}{pz_\mu}$ is a local integer for each χ_μ in the block B. As B is of defect d, $p^{\alpha-d}$ divides each z_μ, hence $p^{\alpha-d+1}$ must divide each $a_{\mu i}$, in other words $\frac{a_{\mu i}}{p^{\alpha-d+1}}$ is an integer for each χ_μ in B. Therefore θ_i' is a generalized character where

$$(36) \qquad \theta_i' = \sum_{\mu=1}^{k} \frac{a_{\mu i}}{p^{\alpha-d+1}} = \frac{1}{p^{\alpha-d+1}}\,\theta_i.$$

If θ_i' is restricted to a p-Sylow subgroup $\mathfrak{P}$ of $\mathfrak{g}$, then the restriction must be a generalized character of $\mathfrak{P}$, and therefore

$$(37) \qquad \frac{1}{p^\alpha}\sum\nolimits_{\mathfrak{P}} \theta_i'(G) = a$$

where a is some rational integer. From the definition (36) of θ_i' and from (26) it follows that $\theta_i'(G) = 0$ for all G in $\mathfrak{P}$ except $G = 1$. Hence the sum in (37) reduces to

$$(38) \qquad a = \frac{1}{p^\alpha}\theta_i'(1)$$
$$= \frac{1}{p^{\alpha-d+1}}\frac{1}{p^\alpha}\theta_i(1)$$
$$= \frac{1}{p^{\alpha-d+1}} f_i ,$$

where a is an integer. This however is contrary to the choice of φ_i, as φ_i was picked in such a way that $\frac{1}{p^{\alpha-d+1}} f_i$ is not an integer. Therefore the assumption that (35) is false has led to a contradiction and (33) is proved.

The last part of the theorem is now very simple. If $a_{\mu i} \neq 0$, then

$$(39) \qquad a_{\mu i} = \frac{p^\alpha}{g}\sum_g{}' \overline{\varphi_i(G)}\,\chi_\mu(G)$$
$$= p^\alpha \sum_{j=1}^{k'} d_{\mu j}\frac{1}{g}\sum_g{}' \overline{\varphi_i(G)}\,\varphi_j(G)$$
$$= p^\alpha \sum_{j=1}^{k} d_{\mu j}\gamma_{ij} \neq 0.$$

Hence there is some j such that $d_{\mu j} \neq 0$ and $\gamma_{ij} = 0$. By Theorem 6.1, this implies that χ_μ, φ_j and φ_i are all in the same block. The converse of this is an immediate consequence of (33).

From the fact that $\frac{a_{\mu i}}{z_\mu}$ is a local integer follows

<u>Corollary 8.2:</u> <u>If</u> φ_i <u>belongs to a block</u> B <u>of defect</u> d, <u>then</u> θ_i'' <u>is a generalized character where</u> θ_i'' <u>is defined by</u>

$$(40) \qquad \theta''_i(G) = p^d\varphi_i(G) \quad \text{if } G \text{ is p-regular}$$
$$= 0 \quad \text{if } G \text{ is p-singular.}$$

In analogy to (29) we will now define another set of numbers as follows,

$$(41) \qquad b_{\mu\nu} = \frac{1}{g'}\sum'_g \chi_\mu(G)\,\overline{\chi_\nu(G)}$$

where $\mu, \nu = 1, \ldots k$. Combining (14) and (29) yields

$$(42) \qquad b_{\mu\nu} = \sum_{i=1}^{k'} d_{\mu i}a_{\nu i}$$
$$= \sum_{i=1}^{k'} d_{\nu i}a_{\mu i}.$$

This shows that $b_{\mu\nu}$ is always an integer, and that $\frac{b_{\mu\nu}}{z_\mu}$ is a local integer. Furthermore (32), (39) and (42) give that for any φ_j in B

$$(43) \qquad \frac{b_{\mu\nu}}{z_\nu} \equiv \sum_{i=1}^{k'} d_{\mu i}\frac{a_{\nu i}}{z_\nu}$$
$$\equiv \sum_{i=1}^{k'} d_{\mu i}\frac{p^\alpha\gamma_{ij}}{f_j}$$
$$\equiv \frac{a_{\mu j}}{f_j} \pmod{p}$$

Now we can prove the following

<u>Corollary 8.3</u>: <u>If</u> χ_μ, χ_ν <u>and</u> χ_ρ <u>are in the same block</u> B, <u>then</u>

$$(44) \qquad \frac{b_{\mu\nu}}{z_\nu} \equiv \frac{b_{\mu\rho}}{z_\rho} \pmod{p}.$$

<u>Furthermore, if</u> $p^{\alpha-d+1}$ <u>does not divide</u> z_μ, <u>then</u> $b_{\mu\nu} \neq 0$

<u>if and only if</u> χ_ν <u>is in</u> B. <u>Actually in this case</u> $\frac{b_{\mu\nu}}{z_\nu} \not\equiv 0$ (mod p).

Proof: The relation (44) follows immediately from (43).

If φ_i is chosen such that $p^{\alpha-d+1}$ does not divide f_i, then $\frac{a_{\mu i}}{f_i} \not\equiv 0$ (mod p). If this were not the case then $\frac{a_{\mu i}}{z_\mu} \equiv 0$ (mod p) as $p^{\alpha-d}$ is the exact power of p dividing both f_i and z_μ. However this would contradict Theorem 8.1. Hence $\frac{a_{\mu i}}{f_i} \not\equiv 0$ (mod p), and this combined with (43) yields the "if" part of the corollary.

To prove the converse, we combine (39) with (42) to get that

$$b_{\mu\nu} = \sum_{i=1}^{k'} d_{\nu i} a_{\mu i} \tag{45}$$

$$= p^\alpha \sum_{i=1}^{k'} \sum_{j=1}^{k'} d_{\nu i} d_{\mu j} \gamma_{ij}.$$

By Theorem 6.1, $d_{\nu i} d_{\mu j} \gamma_{ij} \neq 0$ only when χ_μ, φ_i, φ_j, χ_μ are all in B. If χ_μ and χ_ν are in different blocks then every such term is zero, and in particular $b_{\mu\nu} = 0$.

9. <u>The Number of Characters in a Block</u>.

We are almost in a position now to prove the main theorem on the number of characters in a block. The following result is still necessary.

<u>Lemma 9.1</u>: (I) $\sum_{\mu=1}^{k} a_{\mu i} a_{\mu j} = p^{2\alpha} \gamma_{ij}$

(II) $\sum_{\mu=1}^{k} b_{\mu\nu} b_{\mu\rho} = p^\alpha b_{\nu\rho}$

Proof: From the definition (27) and the orthogonality relations it is an easy consequence that

$$(46) \qquad \sum_{\mu=1}^{k} a_{\mu i} a_{\mu j} = \frac{1}{g} \sum_{\mathcal{G}} \theta_i(G) \overline{\theta_j(G)}$$
$$= \frac{p^{2\alpha}}{g} \sum_{\mathcal{G}}' \varphi_i(G) \overline{\varphi_j(G)}$$
$$= p^{2\alpha} \gamma_{ij}.$$

This proves (I).

The equation (42) connecting $b_{\mu\nu}$ with $a_{\mu i}$ can be used to derive (II) from (I).

$$(47) \quad \sum_{\mu=1}^{k} b_{\mu\nu} b_{\mu\rho} = \sum_{\mu=1}^{k} \sum_{i=1}^{k'} \sum_{j=1}^{k'} d_{\nu i} a_{\mu i} d_{\rho j} a_{\mu j}$$
$$= \sum_{i=1}^{k'} \sum_{j=1}^{k'} d_{\nu i} d_{\rho j} p^{2\alpha} \gamma_{ij}$$
$$= \sum_{i=1}^{k'} d_{\nu i} p^{\alpha} a_{\rho i} = p^{\alpha} b_{\nu\rho} .$$

The following result now becomes almost a triviality.

Theorem 9.2: The number x of irreducible characters in a block B of defect d satisfies both the inequalities,

(I) $\qquad x \leq p^{2d} \gamma_{ij},$

(II) $\qquad x \leq \sum_{\mu=1}^{k} \left(\frac{b_{\mu\nu}}{p^{\alpha-d}}\right)^2 = p^d \frac{b_{\nu\nu}}{p^{\alpha-d}} ,$

where φ_i and χ_ν are so chosen that $p^{\alpha-d+1}$ does not divide either f_i or z_ν.

Proof: If φ_i is chosen as in the theorem, then by Theorem 8.1 $\frac{a_{\mu i}}{p^{\alpha-d}}$ is a non-zero rational integer for all μ

with χ_μ in the block B. Hence $(\frac{a_{\mu i}}{p^{\alpha-d}})^2$ is a positive integer for each χ_μ in B. In particular

$$(48) \qquad 1 \leq (\frac{a_{\mu i}}{p^{\alpha-d}})^2,$$

for all characters χ_μ in B. Hence, by the previous Lemma, on summing (48) over all characters in B we get

$$(49) \qquad x \leq \sum_{\mu=1}^{k} \frac{a_{\mu i}^{\,2}}{p^{2\alpha-2d}} = \frac{p^{2\alpha}\gamma_{ij}}{p^{2\alpha-2d}} = p^{2d}\,\gamma_{ii}.$$

In the same way the number x of characters in B satisfies

$$(50) \qquad x \leq \sum_{\mu=1}^{k} \frac{b_{\mu\nu}^{\,2}}{p^{2\alpha-2d}} = \frac{p^{\alpha}\,b_{\nu\nu}}{p^{2\alpha-2d}} = p^{d}\,\frac{b_{\nu\nu}}{p^{\alpha-d}}\,.$$

This proves both (I) and (II).

We can now give the proof of Theorem 7.1.

The term $\frac{b_{\nu\nu}^2}{p^{2\alpha-2d}}$ occurs in the sum in the inequality of Theorem 9.2 (II). Therefore we can write

$$(51) \qquad x - 1 \leq p^{d}\,\frac{b_{\nu\nu}}{p^{\alpha-d}} - \frac{b_{\nu\nu}^2}{p^{2\alpha-2d}}\,.$$

Let us now write

$$(52) \qquad b = \frac{1}{p^{d}}\,\frac{b_{\nu\nu}}{p^{\alpha-d}}\,.$$

Equation (51) becomes

$$(53) \quad x - 1 \leq p^{d}(p^{d}b) - (p^{d}b)^2 = p^{2d}(b - b^2).$$

It is easily verified that the maximum value of the function $b - b^2$ is $\frac{1}{4}$, hence from (53) we get

$$(54) \qquad x - 1 \leq \frac{p^{2d}}{4}.$$

As $x - 1$ is an integer, (25) is an immediate consequence of (54) and Theorem 7.1 is proved.

10. The Decomposition of the Product of Two Characters.

It is well known that if χ_μ and χ_ν are two irreducible characters of $\mathfrak{G}$, then the product $\bar{\chi}_\mu \chi_\nu$ may be written as a sum of irreducible characters. If a character χ_ρ appears in this sum, then χ_ρ is said to be a constituent of $\bar{\chi}_\mu \chi_\nu$.

One of the consequences of the orthogonality relations for characters is that χ_1 is a constituent of $\bar{\chi}_\mu \chi_\nu$ if and only if $\mu = \nu$. Our object in this section is to generalize this result. The methods used here are very similar to those used in the early parts of this chapter, and the same notation will be used. We prove[13]

Theorem 10.1: If φ_i and φ_j are modular characters in a block B of defect d, and if $p^{\alpha-d+1}$ does not divide f_i, then $\bar{\varphi}_i \varphi_j$ contains some modular character which is in B_1 as a constituent.

Proof: Consider

$$(55) \qquad g\gamma_{ij} = \sum_{\mathfrak{G}}' \overline{(\varphi_i(G)} \varphi_j(G)) \varphi_1(G).$$

If no character of B_1 occurs as a constituent of $\bar{\varphi}_i \varphi_j$, then certainly $g\gamma_{ij} = 0$. This follows from the fact[14] that $\gamma_{k1} = 0$

---

[13]A special case of this theorem can be found in [5] p. 579.

[14]See Theorem 6.1.

if φ_k is not in B_1. The fact that $\gamma_{ij} \neq 0$ is an immediate consequence of Theorem 8.1, because from relations (32) and (33) we get

$$\text{(56)} \qquad \frac{g\,\gamma_{ij}}{f_j} \not\equiv 0 \pmod p.$$

This proves the desired result.

We have also proved

<u>Corollary 10.2</u>: <u>Under the hypotheses of Theorem 10.1</u>, $\gamma_{ij} \neq 0$.

<u>Corollary 10.3</u>: <u>If</u> χ_μ <u>and</u> χ_ν <u>are characters in a block</u> B <u>of defect</u> d, <u>and if</u> $d_{\mu i} \neq 0$ <u>for some</u> φ_i, <u>such that</u> $p^{\alpha-d+1}$ <u>does not divide</u> f_i, <u>then</u> $\bar{\chi}_\mu \chi_\nu$ <u>contains a constituent</u> χ_ρ <u>which is in the block</u> B_1.

Proof: From equation (14) we get, that

$$\text{(57)} \qquad \bar{\chi}_\mu \chi_\nu = \sum_{i,j=1}^{k'} d_{\mu i} d_{\nu j} \bar{\varphi}_i \varphi_j$$

for all p-regular elements of $\mathfrak{G}$. By Theorem 10.1 $\bar{\varphi}_i \varphi_j$ contains a modular character in the block B_1 as a constituent, where φ_j is any modular character in B. As all the coefficients of all modular characters in the expansion of the sum in (57) are positive, $\bar{\chi}_\mu \chi_\nu$ when considered as a sum of modular characters contains some constituent of the block B_1. Now if $\bar{\chi}_\mu \chi_\nu$ is written as a sum of ordinary characters, some constituent must necessarily occur which contains the given modular character of B_1 as a summand. Hence this constituent must lie in B_1.

Corollary 10.4: If χ_μ and χ_ν are characters in a block B of defect d such that $p^{\alpha-d+1}$ does not divide the degree z_μ of χ_μ, then some constituent of $\bar{\chi}_\mu \chi_\nu$ must be in the block B_1.

Proof: If $\chi_\mu = \sum_{i=1}^{k} d_{\mu i} \varphi_i$ for p-regular elements, then $z_\mu = \sum_{i=1}^{k} d_{\mu i} f_i$. As $p^{\alpha-d+1}$ does not divide z_μ, it cannot divide every f_i with $d_{\mu i} \neq 0$. Hence the result follows from Corollary 10.3.

Another result on the decomposition of characters, more special than Theorem 10.1 is the following.

Theorem 10.5: If φ_i is a modular character in the block B_1, and φ_j is a modular character in some block B such that p divides neither of the degrees f_i or f_j, then $\varphi_i \bar{\varphi}_j$ contains a character of the block B as a modular irreducible constituent.

Proof: We define a by the equation

$$(58) \qquad a = \sum\nolimits_{\mathfrak{g}}' \left(\varphi_i(G) \overline{\varphi_j(G)} \right) \varphi_j(G)$$

By Theorem 6.1 it is sufficient to show that $a \neq 0$. This follows from the congruences

$$\begin{aligned}(59) \qquad a &\equiv f_i \sum\nolimits_{\mathfrak{g}}' \frac{h(G)\varphi_i(G)}{f_i} \overline{\varphi_j(G)}\, \varphi_j(G) \\ &\equiv f_i \sum\nolimits_{\mathfrak{g}}' h(G) \overline{\varphi_j(G)}\, \varphi_j(G) \\ &\equiv f_i g \gamma_{ij} \pmod{\mathfrak{p}},\end{aligned}$$

where the summations in (59) are taken over the p-regular classes in $\mathfrak{g}$. By hypothesis $f_i \not\equiv 0 \pmod{p}$ and by

Theorem 8.1 $g\gamma_{ij} \not\equiv 0 \pmod{p}$ as $f_j \not\equiv 0 \pmod{p}$. Hence $a \not\equiv 0 \pmod{p}$ and the theorem is proved.

Corollary 10.6: If χ_μ is in the block B_1, and χ_ν is in some block B such that both χ_μ and χ_ν have a modular irreducible constituent whose degree is prime to p, then $\bar{\chi}_\mu \chi_\nu$ contains at least one character of B as a constituent.

Proof: The proof here is essentially the same as that of Corollary 10.3.

Corollary 10.7: If χ_μ is in B_1 and χ_ν is in some block B such that p does not divide either of the degrees z_μ or z_ν then $\bar{\chi}_\mu \chi_\nu$ contains some constituent which is in B.

Proof: This is immediate from Corollary 10.6.

CHAPTER III

11. A Conjecture of Frobenius.

In this chapter we will use the following notation,

(60) $g = qm$, where $(q,m) = 1$.

The set of all elements in $\mathcal{G}$ of order dividing m will be denoted by $\mathcal{M}$, in symbols

(61) $$\mathcal{M} = \{G : G^m = 1\}.$$

In 1907 Frobenius proved the following

Theorem 11.1: *The number of elements in $\mathcal{M}$ is a multiple of m.*

He furthermore conjectured[15] that if $\mathcal{M}$ contains exactly m elements, then $\mathcal{M}$ is a normal subgroup of $\mathcal{G}$. The normality of $\mathcal{M}$ is of course obvious from the definition, the difficulty arises in trying to prove that $\mathcal{M}$ is a subgroup. Frobenius was able to prove the following two special cases of his conjecture.

Theorem 11.2: *Let $\mathcal{Q}$ be the set of all elements in $\mathcal{G}$ of order dividing q, and $\mathcal{M}$ as defined by (61). If $\mathcal{Q}$ contains exactly q elements and $\mathcal{M}$ contains exactly m elements, then both $\mathcal{Q}$ and $\mathcal{M}$ are normal subgroups of $\mathcal{G}$.*

[15]See [7]. Actually Frobenius proved a more general theorem and made a correspondingly more general conjecture. Proofs of Theorem 11.1 may be found in [4] p. 374, or [12] p. 28.

Hence $\mathcal{G} = \mathcal{Q} \times \mathcal{M}$.

The proof of this theorem is not very difficult and depends on the fact that there are only $qm = g$ products of the form QM, with Q in $\mathcal{Q}$, and M in $\mathcal{M}$. Every element in $\mathcal{G}$ may be written in the form QM, where Q and M commute with each other. As there are exactly g elements in $\mathcal{G}$, this shows that every element of $\mathcal{Q}$ commutes with every element of $\mathcal{M}$. From here on the proof is fairly routine and the theorem can be derived from an investigation of the centralizer of $\mathcal{M}$.

The second special case of this conjecture is much more difficult to prove. Although efforts have been made to prove this without using the theory of characters, no one has yet succeeded in doing so. The result may be stated as follows.[16]

Theorem 11.3: If $\mathcal{G}$ contains a subgroup $\mathcal{Q}$ of order q with the properties

(I) $\mathcal{Q}$ is its own normalizer.

(II) The intersection of $\mathcal{Q}$ with any subgroup conjugate to $\mathcal{Q}$ is either $\mathcal{Q}$ or the group $\{1\}$ consisting of the identity element of $\mathcal{G}$ only.

Then there are exactly $m - 1$ elements not lying in any subgroup conjugate to $\mathcal{Q}$, and these together with the identity element of $\mathcal{G}$ form a normal subgroup of $\mathcal{G}$.

---

[16] The proof of the theorem as originally given by Frobenius may be found in [6] p. 331. An alternative statement of the theorem in the language of permutation groups may be found in [6] p. 334. Burnside was able to give a very elementary proof of the theorem, under the assumption that q is even, this may be found in [6] p. 172.

It is not necessary to assume that $(q,m) = 1$, as this can easily be verified from the other hypotheses. Hence the theorem is an immediate consequence of the conjecture made above.

The only previously known proof of this theorem is the one due to Frobenius. It depends on a very ingenious argument, the crux of which is the fact that the sum of squares of a certain set of rational integers equals one. If hypothesis (I) in Theorem 11.3 is dropped, and we denote the order of the normalizer of $\mathfrak{Q}$ by qt, then in Frobenius' argument the above mentioned sum of squares equals t. This latter result is of course worthless. The main theorem of this chapter may roughly be stated as Theorem 11.3 with hypothesis (I) deleted. We actually prove the more general result.

Theorem 11.4: *Let* $g = qm$ *with* $(q,m) = 1$. *Suppose that the set* $\mathfrak{M}$ *of all elements of order dividing* m *contains exactly* m *elements. Furthermore, assume that there exists a subgroup* $\mathfrak{H}$ *of* $\mathfrak{G}$ *of order* $h = qs$, *such that* $(s,\frac{m}{s}) = 1$, *and such that* $\mathfrak{H}$ *has the properties,*

(I) $\mathfrak{H}$ *contains a normal subgroup* γ *of order* s.

(II) *The intersection of* $\mathfrak{H}$ *with any subgroup conjugate to*[17] $\mathfrak{H}$ *is either* $\mathfrak{H}$ *or is contained in* γ.

Then $\mathfrak{M}$ *is a normal subgroup of* $\mathfrak{G}$.

---

[17] I had originally assumed that the intersection of $\mathfrak{H}$ with any subgroup of order h is either $\mathfrak{H}$ or is contained in γ. I am indebted to Professor Brauer for pointing out to me that my proof goes through in this more general case.

The theorem as stated here is actually a necessary and sufficient condition for $\mathfrak{M}$ to be a normal subgroup of $\mathfrak{G}$, for if $\mathfrak{M}$ is a normal subgroup of $\mathfrak{G}$, $\mathfrak{H}$ may be taken equal to $\mathfrak{G}$.

By letting $s = 1$ in Theorem 11.3 we get the following generalization of Frobenius' result.

Corollary 11.5: Let $g = (q,m)$, with $(q,m) = 1$. Suppose that the set $\mathfrak{M}$ of elements whose order divides m, contains exactly m elements. If there exists a subgroup $\mathfrak{Q}$ of $\mathfrak{G}$ of order q, such that the intersection of $\mathfrak{Q}$ with any subgroup conjugate to $\mathfrak{Q}$ is either $\mathfrak{Q}$ or $\{1\}$, then $\mathfrak{M}$ is a normal subgroup of $\mathfrak{G}$.

Not only are the results above more general than Theorem 11.3, but the proofs are actually shorter and, we hope, more transparent. This is not surprising in view of the fact that we have a very powerful tool in Theorem 3.3 which was not available to Frobenius.

To prove Theorem 11.4 it will be necessary to use the following result due to Schur.[18]

Theorem 11.6: If $\mathfrak{G}$ contains a normal subgroup $\mathfrak{A}$ whose order and index are relatively prime, then there exists a subgroup of $\mathfrak{G}$ which is isomorphic to the factor group $\frac{\mathfrak{G}}{\mathfrak{A}}$. In particular the order of this subgroup equals the index of $\mathfrak{A}$ in $\mathfrak{G}$.

Several attempts have been made to prove Frobenius' Theorem without using character theory. Under the assumption

[18]See [12] p. 132.

that the group $\mathfrak{Q}$ in Theorem 11.3 is solvable, this has actually been done.[19] From Theorem 11.6 it follows that the group $\mathfrak{H}$ of Theorem 11.4 contains a subgroup $\mathfrak{Q}$ of order q. If we assume that $\mathfrak{Q}$ is solvable, then we can avoid the use of character theory in the proof of Theorem 11.4. Theorem 3.3 is in this case replaced by the following result, which is a corollary of Theorem 3.3 but may also be proved without character theory.[20]

Theorem 11.7: Let $\mathfrak{H}$ be a subgroup of $\mathfrak{G}$, $\mathfrak{H}^*$ the subgroup of $\mathfrak{H}$ generated by all products $H_1H_2^{-1}$, where H_1 and H_2 are elements of $\mathfrak{H}$ which are conjugate in $\mathfrak{G}$, if the order and index of $\mathfrak{H}$ are relatively prime, then there exists a normal subgroup $\mathfrak{D}$ of $\mathfrak{G}$ such that

$$\frac{\mathfrak{G}}{\mathfrak{D}} \approx \frac{\mathfrak{H}}{\mathfrak{H}^*}$$

where $\approx$ denotes isomorphism onto.

In Section 14 we conclude this chapter by investigating the conjecture when $q = p^\alpha$. In this case we have the theory of modular character at our disposal and can thus get some results which cannot be proved in the more general case.

12. Some Lemmas.

In this section we prove several lemmas which will be used in the proof of Theorem 11.4, we use the same notation as in that theorem.

[19] See [10].

[20] See either [4] p. 371 and footnote 8 on that page, or see [8], p. 496.

For convenience, we will introduce a notation for the set theoretic difference of two sets $\mathfrak{A}$ and $\mathfrak{B}$, $\mathfrak{A} - \mathfrak{B}$ denotes the set of all elements in $\mathfrak{A}$ which are not in $\mathfrak{B}$. It is not assumed that $\mathfrak{B}$ is contained in $\mathfrak{A}$.

Let $\mathfrak{N}$ be the normalizer of $\mathfrak{H}$, $\mathfrak{N}$ has order

$$n = ht = qst.$$

Lemma 12.1: Under the hypotheses of Theorem 12.4, every element of $\mathfrak{G} - \mathfrak{M}$ is in the normalizer of a subgroup conjugate to $\mathfrak{H}$.

Proof: If G is not in $\mathfrak{M}$, then there is a prime p which divides q and such that some power of G has order p, G necessarily commutes with this power of G. In other words, there is an element P in $\mathfrak{G}$ of order p such that $PG = GP$, or

$$P = G^{-1}PG. \tag{62}$$

The element P is in some p-Sylow group $\mathfrak{P}_1$ of $\mathfrak{G}$. Let $\mathfrak{P}$ be a p-Sylow group of $\mathfrak{H}$, then $\mathfrak{P}$ must be a p-Sylow group of $\mathfrak{G}$, and therefore there exists an element A in $\mathfrak{G}$ such that

$$P \in \mathfrak{P}_1 = A\mathfrak{P}A^{-1} \subset A\mathfrak{H}A^{-1} = \mathfrak{H}_1. \tag{63}$$

The equations (62) and (63) imply that

$$P = G^{-1}PG \in \mathfrak{H}_1 \cap G^{-1}\mathfrak{H}_1G. \tag{64}$$

The hypotheses of Theorem 11.4 state that if $\mathfrak{H}_1$ is distinct from $G^{-1}\mathfrak{H}_1G$ then the intersection of the two groups is of order s and thus cannot contain P. Therefore $\mathfrak{H}_1$ and $G^{-1}\mathfrak{H}_1G$ cannot be distinct, or in other words, G is in the normalizer of $\mathfrak{H}_1$ which is conjugate to $\mathfrak{H}$. This proves the lemma.

Lemma 12.2: The number of elements in $\mathfrak{N} \cap \mathfrak{M}$ is exactly st, and these elements form a normal subgroup $\mathfrak{S}$ of $\mathfrak{N}$. The intersection of $\mathfrak{N}$ with any subgroup conjugate to $\mathfrak{N}$ contains only elements of $\mathfrak{M}$.

Proof: By Theorem 11.1, the number of elements in $\mathfrak{N} \cap \mathfrak{M}$ is a multiple of st, hence greater than or equal to st. Therefore

(65) the number of elements in $\mathfrak{N} - \mathfrak{M}$ is $\leq qst - st$.

The number of groups conjugate to $\mathfrak{N}$ is $\frac{g}{qst}$, as it is easily seen that $\mathfrak{N}$ is its own normalizer. By Lemma 12.1, every element of $\mathfrak{G}$ which is not in $\mathfrak{M}$ lies in one of these conjugate subgroups, this gives

(66) the number of elements in $\mathfrak{G} - \mathfrak{M}$ is

$$\leq \frac{g}{qst}(qst - st) = g - \frac{g}{q} = g - m.$$

By hypothesis, the number of elements in $\mathfrak{G} - \mathfrak{M}$ is exactly $g - m$. Hence it follows that we must have equality in (65), and that no element can be counted twice in (66), that is to say that the intersection of $\mathfrak{N}$ with any subgroup conjugate to $\mathfrak{N}$ contains only elements in $\mathfrak{M}$.

It now only remains to prove that the st elements of order dividing st in $\mathfrak{N}$ form a normal subgroup of $\mathfrak{N}$.

The group $\mathfrak{N}$ contains the normal subgroup $\mathfrak{H}$ of order $h = qs$. It follows from the choice of s, that $(qs,t) = 1$. Now we may apply Theorem 11.6, and this yields[21]

[21] In the special case that $s = 1$, Schur's theorem may be avoided and instead we could use Theorem 11.2. However I have seen no way of doing this in the more general case treated here.

that $\mathcal{N}$ contains a subgroup $\mathcal{T}$ of order t. It is easily seen that $\mathcal{S}$ is a normal subgroup of $\mathcal{N}$, hence $\mathcal{L} = \mathcal{S}\mathcal{T}$ is a group. It is obvious that the order of $\mathcal{L}$ is st, and as there are only st elements of order dividing st in $\mathcal{N}$, $\mathcal{L}$ is a normal subgroup of $\mathcal{N}$.

<u>Lemma 12.3</u>: <u>Let</u> G_1 <u>and</u> G_2 <u>be two elements of</u> $\mathcal{N} - \mathcal{M}$. <u>If</u> G_1 <u>and</u> G_2 <u>are conjugate in</u> $\mathcal{G}$, <u>then they are also conjugate in</u> $\mathcal{N}$.

Proof: Suppose that $GG_2G^{-1} = G_1$, with G in $\mathcal{G}$, then

$$G_1 = GG_2G^{-1} \in \mathcal{N} \cap G\mathcal{N}G^{-1}. \tag{67}$$

If $\mathcal{N}$ and $G\mathcal{N}G^{-1}$ are distinct, then an element G of $\mathcal{N} - \mathcal{M}$ is in the intersection of $\mathcal{N}$ with a group conjugate to $\mathcal{N}$, this contradicts Lemma 12.1, hence $\mathcal{N} = G\mathcal{N}G^{-1}$. Therefore G is in the normalizer of $\mathcal{N}$. As $\mathcal{N}$ is its own normalizer, G must be in $\mathcal{N}$, as was to be proved.

13. <u>The Proof of the Main Theorem</u>.

We will give two proofs of Theorem 11.4, one under the assumption that a subgroup $\mathcal{Q}$ of $\mathcal{H}$, of order q is solvable. The proof in this case will be independent of the theory of characters. We first prove Theorem 11.4 without any additional restrictions.

Let Z be an irreducible representation of $\mathcal{N}$ which contains the normal subgroup $\mathcal{L}$ in its kernel, $\mathcal{L}$ is the group defined in Lemma 12.2. Then Z is a representation of $\frac{\mathcal{N}}{\mathcal{L}}$. Let χ be the character of Z, χ is a function on $\mathcal{N}$ such that if G is in $\mathcal{L}$, $\chi(G) = \chi(1) = z$. We will now extend the domain of definition of χ to the whole group $\mathcal{G}$. By Lemma 12.1, every element of $\mathcal{G}$ is either in $\mathcal{M}$ or is conjugate to some element in $\mathcal{N}$. With this in mind we define

$$(68) \qquad \begin{aligned} \chi(G) &= z \quad \text{if } G \text{ is in } \mathcal{M} \\ \chi(G) &= \chi(N) \text{ if } G = HNH^{-1}, \text{ where } N \text{ is in } \mathcal{N} - \mathcal{M}. \end{aligned}$$

It is not yet clear that χ is a single valued function under this definition. The only thing that needs to be proved is that if $G = H_1N_1H_1^{-1} = H_2N_2H_2^{-1}$, then $\chi(N_1) = \chi(N_2)$. This however is an immediate consequence of Lemma 12.3, and the fact that χ is a class function on $\mathcal{N}$. This argument furthermore also shows that χ is a class function on $\mathcal{G}$.

We wish to show that χ defined by (68) is an irreducible character of $\mathcal{G}$, to do this it is sufficient to show that χ satisfies the conditions of Theorem 3.3. It has already been shown that χ is a class function, and therefore satisfies (I). We will now verify (II), that the restriction of χ to any elementary subgroup $\mathcal{E}$ is a generalized character. For this purpose it is necessary to consider two cases depending on the structure of $\mathcal{E}$.

Case (i) $\mathcal{E} = \mathcal{A}_1 \times \mathcal{A}_2 \times \mathcal{P}$, where $\mathcal{A}_1$ is cyclic of order a_1 dividing m, $\mathcal{A}_2$ is cyclic of order a_2 dividing q, and $\mathcal{P}$ is a p-group, with p dividing m.

Case (ii) $\mathcal{E} = \mathcal{A}_1 \times \mathcal{A}_2 \times \mathcal{P}$, where $\mathcal{A}_1$ and $\mathcal{A}_2$ are as in Case (i) and now $\mathcal{P}$ is a p-group of order dividing q.

It is clear that every elementary group $\mathfrak{E}$ may be written in one of the above ways.

Case (i). The cyclic group $\mathfrak{A}_2$ belongs to some group conjugate to $\mathfrak{N}$. We may assume without any loss of generality that $\mathfrak{A}_2$ is contained in $\mathfrak{N}$, hence χ restricted to $\mathfrak{A}_2$ is the character of the representation Z restricted to $\mathfrak{A}_2$. On the other hand $\chi(G) = z$ if G is in $\mathfrak{A}_1 \times \mathfrak{P}$. Hence χ restricted to $\mathfrak{E}$ is simply the character of a representation of $\mathfrak{E}$ which contains $\mathfrak{A}_1 \times \mathfrak{P}$ in its kernel. In particular, χ restricted to $\mathfrak{E}$ is a generalize character.

Case (ii). The group $\mathfrak{P}$ is contained in some group conjugate to $\mathfrak{N}$, we may assume that $\mathfrak{P}$ is in $\mathfrak{N}$ without any loss of generality. As $\mathfrak{A}_2$ is in the centralizer of $\mathfrak{P}$, it is easily seen[22] that $\mathfrak{A}_2$ lies in $\mathfrak{N}$. Now χ restricted to $\mathfrak{A}_2 \times \mathfrak{P}$ is just the character of the restriction of the representation Z to $\mathfrak{A}_2 \times \mathfrak{P}$. If G is in $\mathfrak{A}_1$, then $\chi(G) = z$. Hence χ restricted to $\mathfrak{E}$ is the character of a representation of $\mathfrak{E}$ which contains $\mathfrak{A}_1$ in its kernel. In particular this restriction to $\mathfrak{E}$ is a generalized character of $\mathfrak{E}$.

We have now verified condition (II) of Theorem 3.3. Condition (III) is trivially true and so it only remains to show that χ satisfies condition (IV).

As χ is an irreducible character of $\mathfrak{N}$, we get

---

[22] This is shown by essentially the same argument as was used in Lemma 12.1.

from the orthogonality relations that

$$(69) \qquad \Sigma_{\mathcal{N}} \chi(G)\overline{\chi(G)} = qst.$$

By Lemma 12.2, $\mathcal{N}$ contains exactly st elements of $\mathcal{M}$, by (68) $\chi(G) = z$ for each such element, hence

$$(70) \qquad \Sigma_{\mathcal{N}-\mathcal{M}} \chi(G)\overline{\chi(G)} = qst - stz^2.$$

Lemma 12.2 also yields the fact that each element of $\mathcal{N} - \mathcal{M}$ occurs in exactly one group conjugate to $\mathcal{N}$, and there are $\frac{g}{qst}$ such conjugate subgroups, hence

$$(71) \qquad \Sigma_{\mathcal{G}-\mathcal{M}} \chi(G)\overline{\chi(G)} = \frac{g}{qst}(qst - stz^2)$$

$$= g - \frac{g}{q}z^2$$

$$= g - mz^2.$$

As $\chi(G) = z$ for each element G in $\mathcal{M}$ and there are m such elements, (71) leads to

$$(72) \qquad \Sigma_{\mathcal{G}} \chi(G)\overline{\chi(G)} = g - mz^2 - mz^2 = g.$$

This finally verifies the last condition of Theorem 3.3, application of this theorem gives the desired result. We have proved

<u>Lemma 13.1</u>: <u>If</u> Z <u>is an irreducible representation of</u> $\mathcal{N}$ <u>which contains</u> $\mathcal{L}$ <u>in its kernel and if</u> χ <u>is the character of</u> Z, <u>then it is possible to extend the definition of</u> χ <u>to the whole group</u> $\mathcal{G}$ <u>by equation (68)</u>. <u>The extended function is then the character of an irreducible representation</u> Z' <u>of</u> $\mathcal{G}$.

Let $\chi_1, \ldots \chi_\rho$ be the set of all irreducible characters of $\frac{\mathfrak{N}}{\mathfrak{L}}$, extend their definition to $\mathfrak{G}$ and consider the irreducible representations $Z_1', \ldots Z_\rho'$ of $\mathfrak{G}$ defined in this way. Define the representation Z' of $\mathfrak{G}$ by

$$Z'(G) = \begin{pmatrix} Z_1'(G) & & 0 \\ & \cdot & \\ 0 & & Z_\rho'(G) \end{pmatrix}$$

where each Z_μ' occurs with multiplicity z_μ. The representation Z' restricted to $\mathfrak{N}$ may be considered as the regular representations of $\frac{\mathfrak{N}}{\mathfrak{L}}$, in particular, the set of matrices $Z'(G)$ contains a subgroup of order q. If G is in $\mathfrak{M}$, then by the definition (68) $\chi_\mu'(G) = z_\mu' = z_\mu$ for $\mu = 1, \ldots \rho$, hence $\chi'(G) = z' = \chi'(1)$, where χ' is the character of Z'. Then by Theorem 1.7, G is contained in the kernel of Z'. These results may be rephrased as follows. The group of matrices $Z'(G)$ is a homomorphic image of $\mathfrak{G}$ which contains a subgroup of order q and contains no elements of order dividing m. Therefore this group must have order q, and in particular the kernel of Z' is a normal subgroup of $\mathfrak{G}$ of order m. As $\mathfrak{M}$ is in the kernel of Z', $\mathfrak{M}$ must be the whole kernel, and hence $\mathfrak{M}$ is a normal subgroup of $\mathfrak{G}$. This finally concludes the proof of Theorem 11.4.

We now proceed to prove Theorem 11.4 under the additional assumption that a subgroup[23] $\mathfrak{Q}$ of $\mathfrak{H}$ of order q is solvable. The proof will not use character theory. The Lemmas from Section 12 will be used, and Theorem 11.7 will be

---

[23]The existence of $\mathfrak{Q}$ is guaranteed by Theorem 11.6. See the remarks after that theorem.

used in place of Theorem 3.3.

We will show that if $q \neq 1$, then there exists a proper normal subgroup of $\mathfrak{G}$, whose order is divisible by m, and which satisfies the hypotheses of Theorem 11.4. After repeated application of this result, we must eventually arrive at a group whose order is divisible by m and for which $q = 1$, this group must then be $\mathfrak{M}$ and the theorem will be proved.

By Lemma 12.3, any two elements of $\mathfrak{H}$ which are conjugate in $\mathfrak{G}$ are also conjugate in $\mathfrak{N}$. Hence the group $\mathfrak{H}^*$ defined in Theorem 11.7 is certainly contained in $\mathfrak{N}'$, where $\mathfrak{N}'$ is the commutator subgroup of $\mathfrak{N}$. By Lemma 12.2, there exists a normal subgroup $\mathfrak{L}$ of $\mathfrak{N}$ such that $\frac{\mathfrak{N}}{\mathfrak{L}} \approx \mathfrak{Q}$, this implies that $\mathfrak{Q}$ is a homomorphic image of $\mathfrak{N}$. As $\mathfrak{Q}$ is solvable by hypothesis, $\mathfrak{Q}$ contains a normal subgroup of prime index, therefore $\mathfrak{N}$ contains a normal subgroup of prime index p, with p dividing q. This shows that $\mathfrak{N}'$ is a proper subgroup of $\mathfrak{N}$ whose index is divisible by p. As $\mathfrak{H}^*$ is contained in $\mathfrak{N}'$, and as q does not divide the order of $\mathfrak{N}'$, $\mathfrak{H}^*$ is a subgroup of $\mathfrak{H}$ whose index is divisible by p. It is easily seen that $\frac{\mathfrak{H}}{\mathfrak{H}^*}$, and hence $\frac{\mathfrak{G}}{\mathfrak{D}}$ is abelian. Now it is easy to show that there exists a normal subgroup $\mathfrak{D}_1$ of $\mathfrak{G}$ containing $\mathfrak{D}$, and such that the index of $\mathfrak{D}_1$ is exactly p.

It can easily be verified that the group $\mathfrak{D}_1$ satisfies the assumption of Theorem 11.4, where $\mathfrak{H}$ is replaced by $\mathfrak{H} \cap \mathfrak{D}_1$. This proves the induction step and thus the theorem.

14. The case $q = p^{\alpha}$.

In this section we investigate a special case of Frobenius' conjecture. We assume that $q = p^{\alpha}$, where p is a prime, and where q is defined by equation (60). The set $\mathfrak{M}$ in this case consists of the p-regular elements of $\mathfrak{G}$. The following result reduces the conjecture to another conjecture, which is stated in the language of the theory of modular characters.

Theorem 14.1: *Let* $g = mp^{\alpha}$, *where* p *is a prime not dividing* m. *If the set* $\mathfrak{M}$ *of p-regular elements of* $\mathfrak{G}$ *consists of exactly* m *elements, and if*[24] $c_{11} \leq p^{\alpha}$, *then* $\mathfrak{M}$ *is a normal subgroup of* $\mathfrak{G}$.

Proof: Let $\theta_1(G)$ be defined as in Section 8, namely

$$\begin{aligned} \theta_1(G) &= p^{\alpha}\varphi_1(G) = p^{\alpha} \quad \text{if } G \text{ is in } \mathfrak{M} \\ &= 0 \quad \text{if } G \text{ is not in } \mathfrak{M}. \end{aligned}$$

Again let[25]

$$\theta_1(G) = \sum_{\mu=1}^{k} a_{\mu 1} \chi_{\mu}(G).$$

If it can be shown that each $a_{\mu 1}$ is a non-negative integer, then by Theorem 1.7 it will follow that $\mathfrak{M}$ is a normal subgroup of $\mathfrak{G}$. We will actually show that under the hypotheses, $a_{\mu 1} = d_{\mu 1}$, $\mu = 1, \ldots k$, where the numbers $d_{\mu 1}$ are the decomposition numbers, and hence each $a_{\mu 1}$ is a non-negative integer. From the definition of the $a_{\mu 1}$ follows

[24] For the definition of c_{11}, see equation (6).

[25] It is rather surprising, but it is not necessary to know that the numbers $a_{\mu 1}$ are integers, this fact is a consequence of the proof of the theorem.

$$\sum_{\mu=1}^{k} a^2_{\mu 1} = \frac{1}{g} \sum_{g} \theta_1(G)\, \overline{\theta_1(G)}$$
$$= \frac{p^{2\alpha}}{g} \sum'_{g} \varphi_1(G)\, \overline{\varphi_1(G)}$$
$$= \frac{p^{2\alpha}}{g}\, m \;=\; p^{\alpha}\, .$$

$\sum_{\mu=1}^{k} d^2_{\mu 1} = c_{11} \leq p^{\alpha}$ by hypothesis. From (17) it also follows that $\sum_{\mu=1}^{k} a_{\mu 1}\, d_{\mu 1} = \frac{1}{g} \sum_{g} \theta_1(G)\, \overline{\Phi_1(G)} = \frac{p^{\alpha}}{g} \sum'_{g} \varphi_1(G)\, \overline{\Phi_1(G)}$ $= p^{\alpha}$.

The Cauchy-Schwartz inequality applied to these sums now yields

$$p^{\alpha} = \sum_{\mu=1}^{k} a_{\mu 1} d_{\mu 1} \leq \sqrt{\sum_{\mu=1}^{k} a^2_{\mu 1} \sum_{\mu=1}^{k} d^2_{\mu 1}} = \sqrt{p^{\alpha} c_{11}} \leq p^{\alpha}.$$

Hence equality must hold above, and this implies that $a_{\mu 1} = d_{\mu 1}$, for each μ, which proves the theorem.

The hypothesis that $c_{11} \leq p$ is satisfied by all groups in which it has been checked. It has been proved for a very large class of groups which includes all solvable groups.[26] It has also been proved true[27] for all groups of order $g = pm$, with p not dividing m.

Independently of the above remarks we can prove a

---

[26] See [5] p. 586. The given class of groups includes all solvable groups because of Hall's theorem. This may be found in [12] p. 133. For solvable groups the conjecture is also an immediate consequence of Hall's Theorem.

[27] See [2] p. 947. It is proved there that $d_{\mu 1} = 1$ or 0 for each μ. This combined with the fact that the number of characters in the block is less than or equal to p (see [3] p. 218) gives the result.

rather special case of the conjecture. It is necessary to use the following known theorem.[28]

Theorem 14.2: If the p-Sylow group $\mathfrak{P}$ of the group $\mathfrak{G}$ is abelian, then there exists a homomorphism from $\mathfrak{G}$ onto the intersection of $\mathfrak{P}$ with the center of the normalizer of $\mathfrak{P}$.

We now prove,

Theorem 14.3: Let $g = p^{\alpha}m$, with p not dividing m. If the set $\mathfrak{M}$ of p-regular elements of $\mathfrak{G}$ contains exactly m elements, and if the p-Sylow group $\mathfrak{P}$ of $\mathfrak{G}$ is cyclic, then $\mathfrak{M}$ is a normal subgroup of $\mathfrak{G}$.

Proof: Let $\mathfrak{A}$ be the unique subgroup of $\mathfrak{P}$ of order p. As all the p-Sylow groups of $\mathfrak{G}$ are conjugate and as each group of order p is characteristic in any Sylow group in which it is contained, all groups of order p are conjugate. Every p-singular element must commute[29] with an element of order p. Therefore every p-singular element of $\mathfrak{G}$ lies in the centralizer of some group which is conjugate to $\mathfrak{A}$. Let $\mathfrak{C}$ denote the centralizer of $\mathfrak{A}$, and $\mathfrak{N}$ the normalizer of $\mathfrak{A}$, and let their orders be respectively c and n. The Sylow group $\mathfrak{P}$ is contained in $\mathfrak{C}$, which in turn is contained in $\mathfrak{N}$. Hence $c = p^{\alpha}c_1$, $n = p^{\alpha}n_1$, where c_1 divides n_1.

The number of p-regular elements in any group conjugate to $\mathfrak{C}$ is a multiple of c_1 by Theorem 11.1, thus we get

---

[28]See [12] p. 143.

[29]This argument is similar to that of Lemma 12.1.

(73) the number of p-singular elements in $\mathfrak{L}$ is $\leq p^{\alpha} c_1 - c_1$.

Any element in the normalizer of $\mathfrak{L}$ must be in the normalizer of $\mathfrak{A}$, therefore the number of groups conjugate to $\mathfrak{L}$ is less than or equal to $\frac{g}{p^{\alpha} n_1}$. We now have

(74) $g - m =$ the number of p-singular elements in $\mathfrak{G}$ is

$$\leq \frac{g}{p^{\alpha} n_1} (p^{\alpha} c_1 - c_1) - (g - m) \frac{c_1}{n_1} \leq g - m.$$

Equation (74) shows that $c_1 = n_1$, and hence that $\mathfrak{L} = \mathfrak{N}$. As $\mathfrak{A}$ is a characteristic subgroup of $\mathfrak{P}$, any element in the normalizer of $\mathfrak{P}$ is also in the normalizer of $\mathfrak{A}$. Therefore the normalizer of $\mathfrak{P}$ is contained in $\mathfrak{N} = \mathfrak{L}$. As $\mathfrak{A}$ is in the center of $\mathfrak{L}$, $\mathfrak{A}$ must lie in the center of the normalizer of $\mathfrak{P}$. Now Theorem 14.2 shows that there exists a proper subgroup in $\mathfrak{G}$ whose index is a power of p. It is clear that such a subgroup will again satisfy the hypotheses of the theorem, and the argument can be repeated. After a finite number of steps it is clear that we will arrive at a subgroup of whose order is m, this must then necessarily be $\mathfrak{M}$ and the theorem is established.

The following rather special result can now be proved by three different methods.

Theorem 14.4: *If g has order pm, where p is a prime not dividing m, and if $\mathfrak{G}$ contains exactly m p-regular elements, then the set $\mathfrak{M}$ of p-regular elements in $\mathfrak{G}$ is a normal subgroup of $\mathfrak{G}$.*

Proof: (i) This is a special case of Corollary 11.5.

(ii) It is known that in this case[30] $c_{11} \leq p$. Hence this follows from Theorem 14.1.

(iii) This is clearly a special case of Theorem 14.3.

[30] See Footnote 27.

BIBLIOGRAPHY

[1] E. Artin, C. J. Nesbitt and R. M. Thrall, Rings with Minimum Condition, Ann Arbor, University of Michigan Press, (1948).

[2] R. Brauer, Investigations on Group Characters, Annals of Mathematics, Vol. 42 (1941), 936-958.

[3] ________, On Blocks of Characters of Groups of Finite Order II, Proceedings of the National Academy of Science, Vol. 32 (1946), 215-219.

[4] ________, A Characterization of the Characters of Groups of Finite Order, Annals of Mathematics, Vol. 57 (1953), 357-377.

[5] R. Brauer and C. J. Nesbitt, On the Modular Characters of Groups of Finite Order, Annals of Mathematics, Vol. 42 (1941), 556-590.

[6] W. Burnside, Theory of Groups of Finite Order, Cambridge University Press, Second Edition, (1911).

[7] G. Frobenius, Ueber einen Fundamentalsatz der Gruppentheorie II, Sitzungsberichte der Preussischen Akademie, Berlin, (1907), 428-437.

[8] D. G. Higman, Focal Series in Finite Groups, Canadian Journal of Mathematics, Vol. 5 (1953), 477-497.

[9] P. Roquette, Arithmetische Untersuchung des Charakterringes einer endlichen Gruppe. Mit Anwendungen auf die Bestimmung des minimalen Darstellungskörpers einer endlichen Gruppe und in der Theorie der Artinschen L-Funktionen, Journal für die Reine und Angewandte Mathematik, Vol. 190 (1952), 148-168.

[10] R. H. Shaw, Remark on a Theorem of Frobenius, Proceedings of the American Mathematical Society, Vol. 3 (1952), 970-972.

[11] B. L. Van der Waerden, Modern Algebra, Vol. II, New York, Frederick Ungar Publishing Company, (1950).

[12] H. Zassenhaus, The Theory of Groups, New York, Chelsea Publishing Company, (1949).

DISTRIBUTION LIST

AGENCY	NO. OF COPIES
Office of Ordnance Research Box CM, Duke Station Durham, North Carolina	10
Office, Chief of Ordnance Washington 25, D. C. ATTN: ORDTB - PS	2
Commanding General Aberdeen Proving Grounds, Md. ATTN: Tech Info Divn	1
Commanding Officer Redstone Arsenal Huntsville, Alabama	1
Commanding Officer Rock Island Arsenal Rock Island, Illinois	1
Commanding General Research and Engineering Command Army Chemical Center, Md.	1
Chief, Ordnance Development Div. National Bureau of Standards Washington 25, D. C.	1
Commanding Officer Watertown Arsenal Watertown 72, Mass.	1
Technical Reports Library SCEL, Evans Signal Corps Lab. Belmar, New Jersey	1
Commanding Officer Engineer Res. and Dev. Laboratories Fort Belvoir, Virginia	1
Commander U. S. Naval Proving Ground Dahlgren, Virginia	1
Chief, Bureau of Ordnance (AD3) Department of the Navy Washington 25, D. C.	1
U. S. Naval Ordnance Laboratory White Oak, Silver Spring 19, Md. ATTN: Library Division	1
Director National Bureau of Standards Washington 25, D. C.	1

DISTRIBUTION LIST (cont.)

AGENCY	NO. OF COPIES
Corona Laboratories National Bureau of Standards Corona, California	1
Commanding Officer Frankford Arsenal Bridesburg Station Philadelphia 37, Penna.	1
Technical Information Service P. O. Box 62 Oak Ridge, Tennessee ATTN: Reference Branch	1
Commanding Officer Signal Corps Engineering Lab. Fort Monmouth, New Jersey ATTN: Director of Research	1
The Director Naval Research Laboratory Washington 25, D. C. ATTN: Code 2021	1
Jet Propulsion Laboratory California Institute of Technology 4800 Oak Grove Drive Pasadena 3, California	1
Director, Applied Physics Laboratory Johns Hopkins University 8621 Georgia Avenue Silver Spring 19, Maryland	1
Chief, Detroit Ordnance District 574 East Woodbridge Detroit 31, Michigan ATTN: ORDEF-IM	2
Commanding General Air University Maxwell Air Force Base, Alabama ATTN: Air University Library	1
Document Service Center U. B. Building Dayton 2, Ohio ATTN: DSC-SD	5

DISTRIBUTION LIST (cont.)

AGENCY	NO. OF COPIES
Commanding General Air Research and Development Command P. O. Box 1395 Baltimore 3, Md. ATTN: RDD	1
Commanding General Air Research and Development Command P. O. Box 1395 Baltimore 3, Md. ATTN: RDR	1
Commander U. S. Naval Ord. Test Station Inyokern China Lake, California ATTN: Technical Library	1
U. S. Atomic Energy Commission Document Library 19th and Constitution Avenue Washington 25, D. C.	1
Scientific Information Section Research Branch Research and Development Division Office, Assistant Chief of Staff, G-4 Department of the Army Washington 25, D. C.	1
Office of Naval Research Washington 25, D. C.	1
Canadian Joint Staff 1700 Massachusetts Ave., N.W. Washington 6, D. C. THRU: ORDGU-SE	1
Commanding General White Sands Proving Grounds Las Cruces, New Mexico	1